

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MAINE

IN THE MATTER OF THE SEARCH OF
THE PERSON OF BENJAMIN BROWN
(DOB xx/xx/1978) AND THE RESIDENCE
OF BENJAMIN BROWN LOCATED AT 10
SPRING STREET, APARTMENT 5,
WATERVILLE, MAINE

No. 1:24-mj-00068-JCN

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Jonathan Duquette, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Task Force Officer with the Federal Bureau of Investigation (FBI). I have been in this position since June 2015. Since January 2018, I have been assigned as a Task Force Officer to the FBI's Boston Division. I am also a Border Patrol Agent with the U.S. Border Patrol and have been in that position since December 2009. In my career, I have utilized various investigative tools and techniques, to include the use of search warrants involving electronic data. Through my employment, I have conducted investigations relating to violations of federal law, including threatening communications.

2. The FBI has jurisdiction to investigate offenses arising under 18 U.S.C. § 875(c), that involve interstate threatening communications.

3. I make this affidavit in support of an application for a search warrant to search the person of Benjamin Brown (DOB xx/xx/1978) and the premises described in the following paragraphs and in Attachment A. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers, other agents, and witnesses. This affidavit is intended to

provide the facts necessary for a determination of probable cause for the requested search warrant.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that a violation of 18 U.S.C. § 875(c) (threatening interstate communications) has been committed by Benjamin Brown, DOB xx/xx/1978. There is also probable cause to search the person and premises described in Attachment A for evidence and instrumentalities of this crime as described in Attachment B.

PERSON AND PROPERTY TO BE SEARCHED

As described in Attachment A, this application is for a warrant to search the person of Benjamin A. Brown (“Brown”), DOB xx/xx/1978. From his Maine driver’s license information, Brown is described as a Caucasian male, weighing 225 pounds, 5’10” tall, with brown hair and brown eyes. From my investigation, which includes reviewing known photographs of Brown, I am familiar with his appearance and will accompany officers during the execution of said warrant. A copy of his photograph on file with the Maine Bureau of Motor Vehicles appears below:



As described in Attachment A, this application is for a warrant to search the premises of 10 Spring Street, Apartment 5, Waterville, Maine (hereinafter “PREMISES”), which is believed to be the residence of and occupied by Brown. I am familiar with this building from the course of my investigation and from a prior interview there in 2023. It is more fully described as light-colored apartment building with the number “10” stamped above the white front door with several apartments inside. Brown’s apartment—Apartment 5—is on the second floor. I will accompany officers during the execution of said warrant. The warrant would also authorize the search of all outbuildings within the curtilage as well as vehicles owned, registered to, or otherwise associated with Brown’s apartment, Apartment 5.

A photograph of the apartment building at 10 Spring Street in Waterville, Maine, from Google Maps appears below:



A photograph of the apartment building at 10 Spring Street in Waterville, Maine, taken by law enforcement on March 5, 2024, appears below:



PROBABLE CAUSE

5. On March 11, 2021, the FBI National Threat Operation Center (NTOC) Social Media Exploitation Team (SOMEX) received a voluntary disclosure from Google LLC's Cyber Crime Investigation Group, indicating that Google/YouTube user by the name of "push een" had posted comments on YouTube threatening to kill Democratic Politicians as well as other individuals. Along with that voluntary disclosure, Google also sent subscriber information for user "push een" which listed the email address of downtownbennybrown1978@gmail.com for that user. Further, Google provided information from Google Payment Corp., showing that user downtownbennybrown1978@gmail.com had the following address information listed in Google Wallet: Benjamin A. Brown, 20 Gold Street, Unit 2, Waterville, Maine, with telephone number 207-307-0211.

6. In Google's disclosure on March 11, 2021, Google included records showing that the above YouTube user "push een" with the email address of downtownbennybrown1978@gmail.com, made the following comments on YouTube videos:

- a. "this is even more of a reason why we need to all own a gun and protect ourselves if that was me I would have shot and killed every fucking pig on my fucking lawn every mother fucker on my lawn would have been dead!!! Look out you fucking pigs because when come on my properly there will be fucking booby traps where I will be able to fucking kill you if you try to fucking fuck with me and my family bitches!!!!" (Posted on March 3, 2021, at 13:51 GMT);
- b. "KILL CHUCK SCHUMER NANCY PELOSI AND JOE BIDEN THEY ARE PURE FUCKING EVIL AND THEY NEED TO FUCKING DIE!!!!!" (Posted on March 03, 2021, at 07:13:47 GMT);
- c. "senator Susan Collins is a fucking cunt I hope that when she's walking to her car one day someone walks up behind her and puts a fucking bullet right in the back of her fucking skull!!!" (Posted on February 16, 2021, at 14:43:52 GMT);
- d. "I have thought an awful lot about killing Joe Biden!!" (Posted on February 16 2021, at 08:16:59 GMT); and
- e. "I can't wait for a revolution so we can burn Washington to the fucking ground!!! Drag Joe Biden out of the White House and beat him to death on his own front lawn!!!!" (Posted on February 15, 2021, at 02:03:05 GMT).

7. Through open-source database research, the FBI was able to confirm that Benjamin A. Brown, DOB xx/xx/1978, SSN xxx-xx-6989, was listed as residing at 20 Gold Street, Apartment 2, in Waterville, ME.

8. On March 22, 2021, an agent with the FBI and an agent with the U.S. Secret Service attempted to make contact with Brown at his last known addresses (20 Gold Street, Apt. 2, Waterville, ME; and 10 Spring St., Apt. 5, Waterville, ME), but they were unsuccessful. On March 22, agents spoke with tenants of apartment 5 on Spring Street and the landlord, and they indicated that Brown did not reside there.¹ On March 25, 2021, an agent with the U.S. Secret Service spoke with Brown's prior landlord at the Gold Street residence, who said he recently evicted Brown in November of 2020, but Brown and his family left before the eviction process was final. The landlord indicated that Brown rented from him for a two-year period before the eviction. The landlord said that during the past year, he found Brown to be increasingly abusive to Brown's family, especially women, and that Brown's wife and kids were subservient to Brown. The landlord did not believe Brown was fascinated with assassins or weapons. He said Brown traveled a lot to see family out of state, and although Brown claimed to have a weapons specialty, the landlord thought this claim was boastful.

9. On April 2, 2021, an agent with the U.S. Secret Service went to 10 Spring Street, Apartment 5, in Waterville and observed a vehicle registered to Brown parked at that residence. On that date, the agent interviewed Brown, who initially denied making the posts but confirmed ownership of the Google user name of "push een" and the email

¹ While unclear, it appears the agents may have gone to the wrong apartment on Spring Street in Waterville.

address downtownbennybrown1978@gmail.com. Brown acknowledged that he “may have” made the posts and said he often gets frustrated by current events and makes exaggerated, hyperbolic posts. Brown said he does not wish harm to anyone listed in his posts and that he primarily uses the YouTube channel Downtown Benny Brown Productions to make posts. Brown also said that he has Tourette’s. Brown said he had no access to weapons or plans to travel. At the conclusion of the interview, Brown was cooperative and apologetic for making the posts. The FBI subsequently closed its investigation in 2021 after referring the matter to the U.S. Secret Service.

10. On April 12, 2023, the FBI NTOC SOMEX team received a voluntary emergency disclosure from Google LLC’s Cyber Crime Investigation Group, indicating that the Google Account fakjoebiden@gmail.com had posted threats to kill George Soros, as well as violent threats against members of the LGBTQ+ community, Mexican politicians, and Alvin Bragg. Google provided the subscriber information for the Google Account fakjoebiden@gmail.com, which showed that the account used the Display Name of John Doe. Google also indicated that the same Android device was used to access the Google account fakjoebiden@gmail.com and the Google account bennybrown6278@gmail.com. Google’s records indicate that the name Benjamin Brown is associated with the fakjoebiden@gmail.com Account, as well as the phone number (207) 289-8613 and the city is listed as Waterville, ME.

11. In that April 12, 2023, emergency disclosure, Google provided the subscriber information for the Google Account bennybrown6278@gmail.com, showing that the display name associated with the account was Hand Hole Productions. The phone number (207)289-8613 was associated with the account. Records from Google

Payment Corp. showed that the following address information was listed in Google Wallet for user bennybrown6278@gmail.com: Benjamin Brown, 10 Spring Street, Apt. 5, Waterville, ME, with phone number (207) 289-8613.

12. In April 2023, the user of the Google Account bennybrown6278@gmail.com posted on other YouTube user's videos. The following are samples of some of the account user's comments provided by Google:

- a. "I'll kill George Soros I'll kill his whole fucking family" (Posted on April 6, 2023, at 3:20 AM PDT);
- b. "GEORGE SOROS NEEDS TO BE ASSASSINATED AND I HAVE NO PROBLEM DOING IT I'LL DO IT FOR FREE" (Posted on April 6, 2023, at 3:20 AM PDT);
- c. "THE PRESIDENT OF MEXICO IS THE LEADER OF THE CARTELS HE HAS A MONSTER HE MUST BE ASSASSINATED!!!" (Posted on April 2, 2023, at 1:07 AM PDT);
- d. "Give me a couple duffel bags of c4 and an automatic pistol with the silencer some grenades and I will take out the cartels myself"; (Posted on April 2, 2023, at 1:02 AM PDT);
- e. "HEY FBI, SORRY TO BE THE BEARER OF BAD NEWS BUT THERE IS NOTHING THAT YOU'LL BE ABLE TO DO TO STOP THE REVOLUTION BECAUSE WE ARE TOO MANY AND WE ARE TOO POWERFUL WE WILL OVERTHROW YOU WE WILL OVERTHROW THE CIA WE WILL OVERTHROW EVERY POLICE OFFICER IN

THIS COUNTRY WHO CHOOSES TO FIGHT ON YOUR SIDE WE WILL
OVERTHROW EVERY SINGLE MILITARY MEMBER WHO CHOOSES
TO FIGHT ON YOUR SIDE WE OUTNUMBER YOU WE OUTGUN YOU
AND YOU WILL NOT WIN!!” (Posted on March 30, 2023, at 8:36 PM
PDT); and

- f. “I AM READY FOR A REVOLUTION AND I HAVE BEEN PREPARING
FOR YEARS ####” (Posted on March 30, 2023, at 8:35 PM PDT).

13. Through investigation, it was learned from open source queries that the
same IP address (2603:7081:6d00:e997:6830:8db0:dace:3aad) was used by both
Google Accounts (fakjoebiden@gmail.com and bennybrown6278@gmail.com).

Through an open-source query for that IP address, it was learned that the IP address
resolves to Winslow, Maine, and service provider Charter Communications, Inc.

Through an advanced open-source query conducted by NTOC for the IP address, it was
learned that it resolved to Waterville, Maine, with provider Spectrum (which operates
as Charter Communications, Inc., in the State of Maine).

14. An open-source search provided several results, some of which were
duplicate entries, under public records for the telephone number (207) 289-8613. The
active phone (meaning the most current result) for the number was listed as belonging
to Benjamin Brown, 10 Spring Street, Apt. 5, Waterville, ME 04901. A query through a
law enforcement database for Benjamin Brown, DOB xx/xx/1978, showed that Brown
was issued a driver’s license in 2021, with an address of 10 Spring Street, Apartment 5,
in Waterville, Maine.

15. On April 13, 2023, I interviewed Brown at 10 Spring Street, Apartment 5, in Waterville, Maine, along with FBI Special Agent Kurt Ormberg. I spoke to a male individual through the closed exterior door of the apartment; therefore, I could not conclusively identify that person as Brown. However, based on the content of the interview and our conversation, I believe it was Brown. I explained to the male who answered the door that I was looking to speak with Benjamin Brown about comments he posted online. During the interview, the person presumed to be Brown said that anything posted online was free speech. The male never said that he was not Brown, and he did not deny posting the comments when I read them to him. Brown said he was only “venting” and did not mean to sound threatening. Brown also claimed that he uses Google voice to text which does not always correctly transcribe what he said. Brown described himself as a peaceful person. Brown was advised to read Title 18, United States Code Section 875(c) for definitions of Interstate Threatening Communications, and he was warned that all statements online do not constitute free speech. Brown acknowledged that he would research the law provided. Brown claimed not to own firearms at that time. In May 2023, the investigation was closed.

16. On February 20, 2024, the FBI National Threat Operations Section (NTOS) Exigent Threat Research and Analysis Crisis Team (EXTRACT) received a voluntary emergency disclosure of information from Google LLC’s Cyber Crime Investigation Group, indicating that Google Account User vnice1937@gmail.com made threats towards immigrants and other elected officials and was stockpiling weapons in preparation for a violent civil war in the United States. Google provided the following subscriber information for the Account vnice1937@gmail.com: display name of

“Ghhgnfhjhvhgv Mvh hc! J! K” and a DOB of “1909.” Google indicated that the Google email account bennybrown6278@gmail.com appeared on the same Android Device as the account vnice1937@gmail.com. Google provided the subscriber information for bennybrown6278@gmail.com, which showed a display name of “JOEBIDEN IS A PEDOPHILE,” a date of birth in 1900, and a telephone number of (207) 289-8613.

17. The following are samples of some of the comments posted by user vnice1937@gmail.com that were provided by Google on February 20, 2024:

- a. “THAT’S RIGHT AND PRETTY SOON WE’RE GOING TO KILL EVERY SINGLE ONE OF YOU WOULD LEGAL IMMIGRANTS YOU’RE ALL GOING TO DIE AT THE HANDS OF OUR GUNS. YOU BROKE INTO THE WRONG COUNTRY AND YOU’RE GOING TO PAY FOR IT WITH YOUR LIFE” (Posted on February 20, 2024, at 4:35 AM PST);
- b. “IF YOU DON’T FIGHT FOR YOUR FREEDOM IT WILL BE TAKEN FROM YOU I CANNOT WAIT TO FIGHT THE CIVIL WAR AND KILL THESE DEMOCRAT POLITICIANS” (Posted on February 15, 2024 at 3:28 UTC);
- c. “ALL OF THESE ILLEGAL IMMIGRANTS DESERVE TO DIE THEY ARE TERRORIST WHO BROKE INTO OUR COUNTRY WE THE PEOPLE HAVE EVERY LEGAL RIGHT TO DEFEND OUR COUNTRY AND KILL THEM ALL AND THAT IS JUST WHAT WE ARE GOING TO DO AND I AM GOING TO BUY ME AN AR-15 TO DO IT” (Posted on February 14, 2024, at 1:42 UTC);

- d. “SADLY PRESIDENT TRUMP WILL NOT BE BACK IN THE WHITE HOUSE BECAUSE THE DEMOCRATS ARE GOING TO STEAL IT. THE ONLY WAY TO SAVE THIS COUNTRY IS A CIVIL WAR OR A REVOLUTION WE MUST TAKE UP ARMS AGAINST THE DEEP STATE GOVERNMENT AND OVERTHROW THEM WITH OUR GUNS BECAUSE THE ONLY WAY TO GET RID OF EVIL IS TO KILL IT”
(Posted on February 7, 2024, at 16:47 UTC);
- e. “I HOPE THE CITIZENS OF DENVER TAKE UP ARMS AGAINST THESE ILLEGAL IMMIGRANTS BECAUSE WE HAVE THAT LEGAL RIGHT THAT’S WHY I’M BY MYSELF LOTS OF GUNS AND I’M GOING TO TAKE UP ARMS AGAINST THESE ILLEGAL IMMIGRANTS” (Posted on February 6, 2024, at 21:49 UTC);
- f. “AT THIS POINT IT’S COMMON SENSE THAT THIS IS NOTHING MORE THAN A POLITICAL ASSASSINATION. DONALD TRUMP IS INNOCENT OF ALL CHARGES THE JUDGES ARE CORRUPT THE WHOLE COUNTRY’S CORRUPT AND WE THE PEOPLE OF THE UNITED STATES OF AMERICA ARE GOING TO START A REVOLUTION A CIVIL WAR AND WE ARE GOING TO OVERTHROW THE CROOKED TIRING GOVERNMENT IN THE FBI AND THE CIA WITH OUR GUNS AND THERE’S NOTHING ANYONE’S GOING TO DO ABOUT IT” (Posted on January 20, 2024, at 2:56 UTC);
- g. “I’M STOCKPILING WEAPONS IN AMMO FOR THE CIVIL WAR SO I CAN KILL AS MANY DEMOCRATS AS POSSIBLE HOPEFULLY

SOMEONE WILL SAVE BARACK HUSSEIN OBAMA FOR ME SO I CAN BLOW HIS FUCKING BRAINS OUT” (Posted on December 25, 2023, at 8:31 UTC); and

- h. “I ALREADY HOPE THIS DOES HAPPEN BECAUSE IT WILL ALLOW ME TO KILL BARACK HUSSEIN OBAMA AND JOE BIDEN IN THE REST OF THE DISGUSTING DEEP STATE DEMOCRATS ALONG WITH THE senator and Governor of MaineE😂😂😂😂😂” (Posted on December 25, 2023, at 8:21 UTC).

18. The following are samples of some of the comments posted by user bennybrown6278@gmail.com that were provided by Google on February 20, 2024:

- a. “AND THIS IS EVEN MORE OF THE REASON WHY WE NEED TO UTILIZE OUR SECOND AMENDMENT RIGHTS START A REVOLUTION AND KILL THE ENTIRE DEEP STATE GOVERNMENT I’M LOOKING FORWARD TO IT I’M GOING TO GO OUT AND BUY AN AR-15 JUST IN CASE ####” (Posted on February 13, 2024, at 1:00 AM PST);
- b. “EVERY SINGLE ONE OF THESE ILLEGAL IMMIGRANTS ARE TERRORISTS THAT BROKE INTO OUR COUNTRY AND WE HAVE EVERY LEGAL RIGHT TO KILL THEM AND THAT’S EXACTLY WHAT I’M GOING TO DO AND THERE IS NOT A GODDAMN PERSON WHO’S GOING TO STOP ME NOT THE FBI NOT THE LOCAL POLICE NOT A MOTHERFUCKING SOUL I FUCKING DARE YOU” (Posted on February 8, 2024, at 8:58 PM PST); and

- c. “I’M GOING TO GO HUNTING FOR THESE ILLEGAL IMMIGRANTS THAT HAVE TALKED TO THESE NEW YORK POLICE OFFICERS I’M GOING TO HUNT THEM DOWN AND KILL THEM” (Posted on February 8, 2024, at 8:53 PM PST).

19. In its February 20, 2024, disclosure, Google stated that records from Google Payment Corp. indicated that the following address information is listed in Google Wallet for user bennybrown6278@gmail.com: Benjamin Brown, 10 Spring Street, Apt. 5, Waterville, ME, with phone number (207) 289-8613.

20. On February 20, 2024, FBI Special Agents (SA) Dale Wengler and Andrew Drewer attempted to interview Benjamin Brown at 10 Spring Street, Apartment 5, Waterville, Maine. Again, the male who answered the door would not open the door, and his identity could not be conclusively confirmed. However, based on the content of the interview and the conversation, SA Wengler and I believe it was him. The agents spoke with the male who is believed to be Brown about his recent posts on YouTube. The male presumed to be Brown acknowledged the posts and said he was not making threats towards others and that he was not going to hurt himself or anyone else because he is not a violent person. The male also said that he did not own a gun and that he would only defend himself if he was threatened. The male believed to be Brown said he would stop posting on YouTube so the agents would not have to come back. The male also acknowledged that agents had admonished him before about making threats.

21. The investigation has shown that Google account users bennybrown6278@gmail.com and vnice1937@gmail.com have been posting threatening comments on YouTube videos as recently as February 20, 2024. According to

information provided by Google on February 20, 2024, in its voluntary emergency disclosure to the FBI NTOS EXTRACT, the bennybrown6278@gmail.com Account is associated with Benjamin Brown of 10 Spring Street, Apt. 5, Waterville, ME, with phone number (207) 289-8613. According to records from Google provided on February 20, 2024, the vnice1937@gmail.com Account is linked to the bennybrown6278@gmail.com Account because the same Android device was used to access both accounts.

22. As indicated above, an open-source search of telephone number (207) 289-8613 produced several results, with the most recent result indicating that the phone number belonged to Benjamin Brown of 10 Spring Street, Apt. 5, Waterville, ME 04901.

23. As a result, there is probable cause to believe that Brown committed the offense of interstate threatening communications in violation of 18 U.S.C. § 875(c). There is also probable cause to search the person and property described in Attachment A for evidence of these crimes as described in Attachment B.

TECHNICAL TERMS

24. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP

addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

25. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

26. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

27. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why,

when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other

evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in

- advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
 - f. I know that when an individual uses a computer to post threatening comments on the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

28. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software,

and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

29. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

30. Because it appears other people may share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant

could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

31. Based on the foregoing, I request that the Court issue the proposed search warrant. Based on the information described above, there is probable cause to believe that evidence and instrumentalities of these crimes, as described in Attachment B, are contained on the person and property described in Attachment A.

Respectfully submitted,




Jonathan Duquette
Task Force Officer
Federal Bureau of Investigation

Sworn to telephonically and signed
electronically in accordance with the
requirements of Rule 4.1 of the Federal Rules
of Criminal Procedure

Date: Mar 06 2024

City and state: Bangor, ME




Judge's signature
John C. Nilsson U.S. Magistrate Judge
Printed name and title